REMARKS

This Amendment is responsive to the final Office Action dated July 12, 2005, in which Claims 1-25 were rejected. Claims 1, 6, 7, 8, 9, 10 and 22 have been amended. Accordingly, Claims 1-25 are pending in the application, and are presented for reconsideration and allowance.

A. Comments related to the response to arguments in paragraphs 1-2 of the final Office Action.

In responding to Applicants' arguments, the final Office Action specifically notes that "these passages (of Silverbrook cited by Applicants) are merely cautionary statements advising one of ordinary skill in the art that when using such a generator, it is vitally important that the initial seed for the generator be created non-deterministically, and ideally should be truly random". Applicants agree with the Examiner on this point, and further emphasize that these cautionary statements are mandatory requirements according to Silverbrook.

However, the Office Action goes on to say that "Silverbrook also teaches a method by which a random seed can be generated non-deterministically *by the Authentication Chip* by means of hashing data from a random test image (col. 204, lines 10-20, italics added)." The cited section from Silverbrook says

> A simple yet useful source of random numbers is the Lavarand ® system from SGI. This generator uses a digital camera to photograph six lava lamps every few minutes. Lava lamps contain chaotic turbulent systems. The resultant digital images are fed into an SHA-1 implementation that produces a 7-way hash, resulting in a 160-bit value from every 7th bye from the digitized image. These 7 sets of 160 bits total 140 bytes. The 140 byte value is fed into a BBS generator to position the start of the output bitstream. The output 160 bits from the BBS would be the key or (sic, for?) the Authentication chip 53.

As with all other sections of Silverbrook dealing with the random seed, this passage refers to a method for generating a random seed from chaotic or random data originating from an event outside of the camera. In the case of the Lavarand ® system from SGI, the chaotic data originates from an image outside of the camera, namely, an image of the different fluids interacting within the Lava Lite® lamps (as explained in the U.S. Patent No. 5,732,138 to Noll et al., which was made of record in the final

Office Action, but not relied upon). As evident from the above paragraph and the cited patent, the Lavarand ® system from SGI requires, for example, a physical setup to power and contain the Lava Lite® lamps. It is obviously not intended to be carried around by a photographer; nor is it intended to be somehow miniaturized – lamps and all - for inclusion in a digital camera.

Consequently, there would appear to be nothing in this paragraph from Silverbrook, or in the general literature about the Lavarand ® system from SGI in the cited patent, that would suggest that the random seed would be generated non-deterministically *by the Authentication Chip* in the Silverbrook camera by means of hashing data from a random test image.

However, whether there is agreement on this point or not, it should be clear that the chaotic condition of the "lava" in the lamps provides the randomness that is essential to the Lavarand ® system from SGI. In contrast, in Applicants' invention the random seed is provided entirely from sensor noise within the digital camera. There is no contribution from an external image, such as an image of six Lava Lite® lamps. Consequently, and this is the big advantage, the entire system and mechanism for the generation of the "initial seed" for the generator can be truly random, and totally contained within the camera.

B. Claim amendments.

Therefore, and to help in distinguishing from systems such as the Lavarand ® system from SGI, independent claims 1, 6, 7, 8, 9, 10 and 22 have been amended to indicate that the improvement includes "a processor located within the digital camera for generating a random seed *entirely from sensor noise within the digital camera*..." (e.g., from amended claim 1, italics added for the addition). This feature is further delineated in the present dependent claims, as for example, wherein present claim 2 recites "further including an image sensor for capturing images, and wherein the processor includes means for producing a random seed for the private key by processing an image captured from the image sensor so that the random noise level in the captured image is used in producing the random seed...". Such a random noise level is produced by random dark field image data taken from the sensor (see, for

example, present claim 24). This random dark field image data taken from the sensor with the shutter closed relates entirely to amplified dark current noise (page 9, line 29 to page 10, line 3 of the specification), which is due to sensor noise within the digital camera.

Since this additional feature has been added to all of the independent claims, claims 1-25 are believed to be allowable over the art of record, whether under 35 USC 102 or 35 USC 103.

C. Specific comments related to the anticipation rejections of claims 22-24 in paragraphs 3-4 of the final Office Action.

Claims 22-24 are rejected under 35 USC 102(e) as being anticipated by Silverbrook (US 6,788,336), specifically citing the aforementioned col. 204, lines 10-20.

As now amended, claim 22 recites "...a processor located within the digital camera for generating the private key from a physically random process entirely based on image sensor noise within the digital camera...". As argued above in section A, the chaotic condition of an external image, e.g., the "lava" in the lamps, provides the randomness that is essential to the Lavarand ® system from SGI, as disclosed in the aforementioned col. 204 of Silverbrook. There is no disclosure in Silverbrook of entirely basing the random process on sensor noise within the digital camera. Therefore, claims 22-24 are believed to be allowable over Silverbrook under 35 USC 102(e).

D. Specific comments related to the obviousness rejections of claims 1-21, and 25 in paragraphs 5-7 of the final Office Action.

Claims 1, 6-21 and 25 are rejected under 35 USC 103(a) as being unpatentable over Safai et al. (US 6,167,469), and further in view of Silverbrook (US 6,788,336).

In this rejection, Safai et al. is characterized as disclosing a processor located within a digital camera for generating a private key and a public key. From an inspection of the patent disclosure, it would appear that the only indication that a key is generated within the camera is a reference in claim 29 to a step of "generating", which comprises "computing and storing a unique private key value...", and in identical language in the "Summary of the Invention" (col. 4, line 11). In both cases, the

generating step occurs in a method claim for a camera. However, the detailed description (see, for example, the description of "Image Authentication" in col. 15, line 60 to col. 16, line 50) is completely silent as to any generation of a key in the camera, saying only that the "private key is stored in the camera" (col. 16, line 29) or "embedded in firmware in the camera" (col. 16, line 32). Consequently, the skilled person would receive no enabling guidance from this patent as to what might be tried in order to implement the step of "computing ... a unique private key value..." as part of a method implemented in the camera.

The Examiner acknowledges that Safai et al. says nothing about generating a random seed and using the random seed to generate a private key and a public key. Therefore. Silverbrook is characterized in the rejection as disclosing a processor located within a digital camera that generates a random seed (citing col. 189, lines 45-55; col. 173, line 35-col. 175, line 2 for random number seed R) and teaches using a random seed R to generate keys (citing col. 151, lines 12-13 and col. 193, line 25-col. 195, line 25). The applicants respectfully disagree with these observations, in particular finding no such teaching or suggestion in Silverbrook that a processor located within a digital camera generates a random seed.

As the Examiner noted, Silverbrook in column 151 says that "random number generators are also often used to generate keys" but then Silverbrook goes on to say (lines 12-13) that "it is therefore best to say at the moment, that all generators are insecure for this purpose". With regard to such a concern for security, Silverbrook says in col. 173, lines 51-52 that "the seed for R must NOT be generated with a computer-run random number generator" (emphasis in original wording in the patent). Likewise, K1 and K2 (the public and private keys) "must NOT be generated with a computer-run random number generator" (col. 189, lines 13-14 and 35-36). Instead, according to Silverbrook, these numbers are physically generated random numbers gathered from a physically random phenomenon, that is, actually generated in a way that is not deterministic, e.g., "to set K1 (or K2), a person can toss a fair coin 160 times, recording heads as 1, and tails as 0" (col. 189, lines 16-19 and 38-39).

As mentioned above in section A, and as cited in the final Office Action, Silverbrook refers to a method for generating a random seed from chaotic data

originating from an event outside of the camera (col. 204, lines 10-20). Specifically, the chaotic data originates from an image outside of the camera, namely, an image of the different fluids interacting within the Lava Lite® lamps. Thus, these citations make it even more clear that Silverbrook teaches unequivocally that an in-camera processor should not be used to generate a random seed.

As now presented, independent claims 1, 6, 7, 8, 9, and 10 have been amended to indicate that the improvement includes "a processor located within the digital camera for generating a random seed *entirely from sensor noise within the digital camera...*" (from amended claim 1, italics added for the amendment). As argued above in section A, the chaotic condition of an external image, e.g., the "lava" in the lamps, provides the randomness that is essential to the Lavarand ® system from SGI, as disclosed in the aforementioned col. 204 of Silverbrook. There is no disclosure in Silverbrook of generating a random seed entirely from sensor noise within the digital camera. Therefore, claims 1 and 6-21 are believed to be allowable over Safai et al. in view of Silverbrook under 35 USC 103(a). Since claim 25 is dependent from claim 22, claim 25 is also believed to be allowable for reasons as stated above in section C concerning its parent claim 22.

Dependent claims 2-5 are rejected under 35 USC 103(a) as being unpatentable over Safai and Silverbrook as applied to claim 1 above, and further in view of Glass et al. (US 6,332,193). Claims 2-5 are dependent on claim 1, and therefore include all the features thereof. Accordingly, for the reasons set forth above with regard to amended claim 1, claim 2-5 are also believed to be patentable. However, notwithstanding the allowability of claims 2-5 for reasons as stated above, Glass et al. does not disclose or suggest anything relating to use of the random noise level in the captured image to produce a random seed – as this is particularly claimed in claims 2 and 3. Furthermore, Glass et al. does not disclose or suggest anything relating to one or more algorithms for producing a random seed, wherein the random seed is used to produce a random number k, and for using the random number k to create the image authentication signature by hashing the raw image data prior to image processing – as this is particularly claimed in claims 4 and 5. Moreover, for reasons as stated above in section A, Silverbrook fails to teach or suggest production of the random seed entirely

from image sensor noise within the digital camera. Accordingly, claims 2-5 are believed to be patentable over the combination of the teaching of Safai et al., Silverbrook and Glass et al.

The remaining references – Noll et al. (US Patent No. 5,732,138) and Scheiner, Bruce "Applied Cryptography" – were not relied upon by the Examiner on their merits in relation to the claims but considered pertinent to applicant's disclosure. They have been considered for purposes of this response but are at most cumulative and not believed to be otherwise relevant.

If there are any formal matters remaining after this response, Applicants' attorney would appreciate a telephone call to attend to these matters.

In view of the foregoing, this application is believe to be in condition for allowance, the notice of which is respectfully requested.

The Commissioner is hereby authorized to charge any fees in connection with this communication to Eastman Kodak Company Deposit Account No. 05-0225. ***A duplicate copy of this communication is enclosed.***

Respectfully submitted,

Pamela R Crocker

Pamela R. Crocker
Attorney for Applicant(s)
Registration No. 42,447

PRC:cjm
Telephone: (585) 477-0553
Facsimile: (585) 477-4646